REMARKS

In accordance with the foregoing, claim 5 is amended. No new matter is being presented, and approval and entry are respectfully requested.

Claims 1-19 are pending and under consideration. Reconsideration is respectfully requested.

Entry Of Amendment Under 37 CFR §1.116

Applicant requests entry of this Rule 116 Response because it is believed that the amendment of claim 5 puts this application into condition for allowance and should not entail any further search by the Examiner since no new features are being added or no new issues are being raised. Claim 5 is amended to correct a typographical error and recite a data generating apparatus includes a generation device that "stores" the irreducible polynomial.

Page 6: Allowable Subject Matter

Claims 1-10 are allowed. (Action at page 6). Applicant appreciates the indications of allowable subject matter.

Pages 2-6: Rejection Of Claims 11-19

Page 2 of the Action indicates that claims 11-12 and 14-19 are listed in the Office Action as being rejected under 35 U.S.C. §103(a) as being unpatentable over Eichelberger et al. (U.S.P. 4,687,988) in view of "math word article (Finite Field)." However, in a telephone conversation between the Applicant's representative and the Examiner, the Examiner confirmed that the present Office Action should instead indicate that claims 11-12 and 14-19 are rejected under 35 U.S.C. §103(a) as being unpatentable over Eichelberger in view of Leppek (U.S.P. 5,933,501) and Schneier (Applied Cryptography, 1996). Accordingly, the current request for reconsideration and traverse of the rejections addresses the same.

Claim 13 is rejected under 35 U.S.C. §103(a) as being unpatentable over Leppek in view of Wright (Paper: A Random Polynomial Generator, July 14, 1994). The rejection is traversed.

Independent claim 11 recites a data generating apparatus "inputting a condition designating a finite field; and an expression data storage device storing expression data of the finite field, wherein the expression data is based on random numbers generated that are based on the inputted condition."

Independent claim 16 recites a method including "designating a condition for a finite field; generating a plurality of random numbers based on the designated condition; generating expression data of the finite field based on the generated random numbers; and storing the

generated designated expression data."

The Action concedes that Eichelberger does not teach "designating a condition for a finite field." (Action at page 2). The Action also concedes that Leppek does not teach the "details that would indicate that the PGP algorithm whose conditions are of a finite field, . . . (and) is silent on the origins of the key and therefore a condition specified by a user." (Action at page 3).

However, the Examiner contends that a modification of Leppek with Schneier teaches recited features of claims 11 and 16 and there is motivation to combine the same since "Schneier gives the details." The Examiner further contends that the motivation for the combination is to give "the user the ability to be as unpredictable as possible." (Action at page 4).

Applicant submits that one of ordinary skill in the art would not look to modify an apparatus for testing very large scale integrated circuit devices as taught by Eichelberger, in a manner as the Examiner contends, so as "to be as unpredictable as possible."

Further, Applicant submits that one of ordinary skill in the art would not look to modify such a testing apparatus as taught by Eichelberger with PGP algorithms taught by Schneier that are used for cryptography without the benefit of appellant's specification. As set forth in MPEP §2144.04:

> (t)he mere fact that a worker in the art could rearrange the parts of the reference device . . . is not by itself sufficient to support a finding of obviousness. The prior art must provide a motivation . . . without the benefit of appellant's specification, to make the necessary changes in the reference device.

In support of the rejection of dependent claims 12, 14-15 and 17-18, the Examiner contends a motivation to modify Eichelberger with Leppek is so the combination would "be a method of using the testing system of Eichelberger to test the system of Leppek."

However, Applicant respectfully points out that Leppek teaches a data processing and communications system (see, for example, col. 3 starting at line 25) where "the present invention resides primarily in what is effectively a prescribed set of communication encryption and decryption software employed by digital data terminal and communication equipment."

Accordingly, Applicant submits that there is no stated motivation to modify software for an apparatus for testing integrated circuit devices as taught by Eichelberger so as to test data terminals and communication equipment, as the Examiner contends.

In support of the rejection of dependent claim 13, the Examiner contends that Wright teaches generating irreducible polynomial data. (Action at page 6).

However, Applicant submits that even an *arguendo* combination of the cited art does not teach automatically generating the expression data of the finite field. That is, a generated polynomial, as taught by Wright, that has coefficients that are assigned in a random manner does not teach a method including an irreducible polynomial, according to an aspect of the present invention.

Summary

Since *prima facie* obviousness is not established, the rejection should be withdrawn and claims 11-19 allowed.

CONCLUSION

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

If there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: April 21, 2006

By: Paul W. Bobowiec

Paul W. Bobowiec
Registration No. 47,431

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501